REMARKS

I. General

Claims 1-22 were pending in the present application, and all of such claims are rejected in the current Office Action (mailed January 31, 2006). The outstanding issues raised in the current Office Action are:

- Claims 1-22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,578,147 to Shanklin et al. (hereinafter "*Shanklin*") in view of U.S. Patent No. 6,279,113 to Vaidya (hereinafter "*Vaidya*").

In response, Applicant respectfully traverses the outstanding claim rejections, and requests reconsideration and withdrawal thereof in light of the remarks presented herein.

II. Rejections Under 35 U.S.C. §103

Claims 1-22 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Shanklin* in view of *Vaidya*. Applicant respectfully traverses this rejection.

To establish a prima facie case of obviousness, three basic criteria must be met. *See* M.P.E.P. § 2143. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the applied references must teach or suggest all the claim limitations. Without conceding any other criteria, the applied references fail to teach or suggest all elements of the claims, and insufficient motivation exists for combining the references in the manner applied.

A. Applied References Fail to Teach or Suggest All Claim Elements

Of the rejected claims, claims 1, 7, 14 and 19 are independent. Applicant respectfully submits that neither *Shanklin* nor *Vaidya* teaches or suggests the limitations of independent claims 1, 7, 14 and 19.

Independent Claim 1

Independent claim 1 recites, in part, "reading a first packet received by the node," "comparing [a] first signature [of the first packet] with a signature file comprising a first machine-readable logic representative of a first packet signature," "reading a second packet generated by the node in response to reception of the first packet," "comparing [a] second signature [of the second packet] with the signature file" and "identifying the first packet as an intrusion if the first signature corresponds with the first machine readable logic and the second signature corresponds with the second machine readable logic" (emphasis added).

The Office Action concedes that *Shanklin* does not explicitly disclose identifying the first packet as an intrusion if the first signature corresponds with the first machine readable logic and the second signature corresponds with the second machine readable logic. *See* page 3 of the Office Action. However, the Office Action asserts that *Vaidya* teaches this element. Applicant respectfully disagrees. The Office Action relies upon column 8, lines 15-39 of *Vaidya* as teaching the above element. Column 8, lines 15-39 of *Vaidya* merely provides:

> A timer/counter based attack signature profile directs the virtual processor 36 to execute instructions associated with a single expression on every data packet associated with a particular application session to determine whether an event has occurred a threshold number of times within a predetermined time interval. For instance, a timer/counter based attack signature profile might direct the virtual processor 36 to execute an instruction associated with the expression "is user Z attempting to access file A?" on every packet associated with a session application Y. The instructions also direct the virtual processor 36 to determine whether the number of attempts user Z makes to access file A exceeds 5 attempts within any 10 minute period. The first packet which the virtual processor 36 recognizes as being associated with an attempt by user Z to access file A causes the virtual processor 36 to activate a timer 37 and to set a counter 35 to one. The timer and counter information are entered into the state cache 44. Each subsequent detection of an attempt by user Z to access file A triggers the virtual processor 36 to access the timer and counter information from the state cache 44 and to determine whether the threshold has been met. If the threshold is met, a network intrusion has been detected and the virtual processor 36 notifies the reaction module 38.

The relied-upon portion of *Vaidya* in no way teaches or suggests identifying the first packet as an intrusion if the first signature corresponds with the first machine readable logic

and the second signature corresponds with the second machine readable logic. Rather, this merely teaches using a counter and/or timer to determine the number of attempted unauthorized accesses during a given time period. *Vaidya* in no way teaches or suggests identifying a packet as an intrusion if a signature of a received first packet corresponds with first machine readable logic and a signature of a second packet that is generated by the node in response to reception of the first packet corresponds with second machine readable logic.

In view of the above, the rejection of claim 1 should be withdrawn.

Independent Claim 7

Independent claim 7 recites "reading a first packet," "comparing [a] first signature [of the first packet] with a first instruction set comprising a first set of machine readable logic representative of a first packet signature," "reading a second packet generated in response to reception of the first packet," "comparing [a] second signature [of the second packet] with a second instruction set comprising a second set of machine readable logic representative of a second packet signature" and "identifying the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic" (emphasis added). As discussed above with claim 1, the combination of *Shanklin* and *Vaidya* fails to teach or suggest at least "identifying the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic". Accordingly, the rejection of claim 7 should be withdrawn.

Independent claim 14

Independent Claim 14 recites a "network filter service provider operable to receive a first packet and . . . and compare [a] first signature [of the first packet] with a first instruction set comprising a first set of machine readable logic representative of a first packet signature," "receive a second packet generated in response to receipt of the first packet and . . . compare [a] second signature [of the second packet] with a second instruction set comprising a second set of machine readable logic representative of a second packet signature" and "identify the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable

logic" (emphasis added). As discussed above with claim 1, the combination of *Shanklin* and *Vaidya* fails to teach or suggest at least "identify the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic". Accordingly, the rejection of claim 7 should be withdrawn.

Independent Claim 19

Independent claim 19 recites "reading a response packet by the node, the response packet generated in response to reception of a first packet by the node," "determining a signature of the response packet," "comparing the signature with a signature file comprising a machine-readable logic representative of a packet signature" and "identifying the first packet as an intrusion if the signature [of the response packet] corresponds with the machine-readable logic" (emphasis added). Applicant respectfully submits that neither *Shanklin* nor *Vaidya* teaches or suggests identifying a first packet received by a node as an intrusion based on a signature of a response packet to the first packet as generally recited by independent claim 19. Thus, at least this reason, Applicants respectfully submit that independent claim 19 is patentable over the cited references.

Dependent Claims

Claims 2-6, 8-13, 15-18, 21 and 22 depend respectively from one of independent claims 1, 7, 14 and 19. For at least the reasons discussed above, independent claims 1, 7, 14 and 19 are in condition for allowance. Therefore, claims 2-6, 8-13, 15-18, 21 and 22 are likewise believed to be allowable at least based on their dependency from their respective independent claim for the reasons discussed above. Accordingly, Applicant respectfully requests that the rejection of claims 1-22 be withdrawn.

B. Insufficient Motivation to Combine References in the Manner Applied

It is well settled that the mere fact that references can be combined or modified is not sufficient to establish a prima facie case of obviousness, *see* M.P.E.P. § 2143.01. Rather, there must have been some explicit teaching or suggestion in the art to motivate one of even ordinary skill to combine such elements so as to create the same invention. *See Arkie Lures,*

Inc. v. Gene Larew Tackle, Inc., 119 F.3d 953, 957, 43 U.S.P.Q.2d 1294 (Fed. Cir. 1997). Here, no such motivation exists to combine the teachings of *Vaidya* with the system of *Shanklin* in the manner suggested by the Office Action. The Office Action asserts that It would have been obvious to combine the teachings of *Vaidya* with *Shanklin* "because comparing both incoming packets to a node and outgoing packets from the same node lowers the chance of false positives because it takes two checks of the same packet (once before being acted upon and once after the packet has been received) before a packet is marked as intrusive." Applicant fails to understand the assertion by the Office Action. Comparing a signature of a first received packet with first machine readable logic and comparing a signature of a second packet that is generated in response to the first received packet with second machine readable logic does not constitute making two checks of the same packet, as asserted by the Office Action. The Office Action appears to assert that double-checking the same packet to lower the chance of false positives is sufficient. This is not what is recited by the claims. Thus, the relied-upon motivation is at best improper for combing the references in the manner applied, and is at worst nonsensical altogether.

Further, the asserted motivation in no way comes from the applied references themselves. That is, the relied upon references provides no motivation for making the two checks of the same packet in the manner asserted by the Office Action. A review of the references indicates that neither makes any mention of false positives, and thus the references provide no motivation for making the drastic change proffered by the Examiner in attempt to lower the chance of false positives. The language of the recited motivation appears to be circular in nature, merely stating that it is obvious to make the modification because it is obvious to achieve the result. That is, the recited motivation merely states that it is obvious to perform the double-checking so that the packets will be double-checked to reduce the chances of false positives. Such language is merely a statement that the *Shanklin* reference can be modified, and does not state any desirability for making the modification. The mere fact that references can be combined or modified does not render the resultant combination or modification obvious unless the prior art also suggests the desirability of the combination or modification. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990), as cited in M.P.E.P. § 2143.01. Thus, the motivation provided by the Examiner is improper, as the cited prior art reference must establish the desirability for making the modification.

For this further reason, the above rejections of claims 1-22 should be withdrawn.

III. Conclusion

In view of the above, Applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 08-2025, under Order No. 10016862-1 from which the undersigned is authorized to draw.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV 568259931US in an envelope addressed to: M/S Amendment, Commissioner for Patents, Alexandria, VA 22313.

Date of Deposit: April 5, 2006

Typed Name: Gail L. Miller

Signature: Gail L. Miller

Respectfully submitted,

By: _____
Jody C. Bishop
Attorney/Agent for Applicant(s)
Reg. No. 44,034
Date: April 5, 2006
Telephone No. (214) 855-8007